CLAIMS

What is claimed is:

1. A method of creating a digital certificate for a user comprising:

deriving a first data set containing data pertaining to the user and useful to an issuing party issuing the digital certificate;

associating a user public key with the first data set thereby creating a second data set, the user public key and a corresponding user private key both generated and authenticated before the creation of a digital certificate by the issuing party;

encrypting the second data set using an issuer private key;

creating a digital certificate containing the user public key, the first data set, and the encrypted second data set, the digital certificate being identifiable by an issuing-party identifier; and

storing the digital certificate at a user-allotted memory segment of a certificate library, in which one or more digital certificates for the user can be stored at the user-allotted memory segment.

2. A method as recited in claim 1 further including associating a certificate chain with the digital certificate, the certificate chain having a trusted root, the trusted root being different from other trusted roots stored at the user-allotted memory segment.

3. A method as recited in claim 2 further including using the Public Key Infrastructure (PKI) to configure the digital certificate and the associated certificate chain, thereby creating one PKI, and storing two or more PKIs at the user-allotted memory segment of the certificate library.

4. A method as recited in claim 2 further including using the Digital Encryption Standard (DES) shared-key system to configure the digital certificate and the associated certificate chain, and storing two or more DES shared-key systems at the user-allotted memory segment of the certificate library.

5. A method as recited in claim 1 further including accessing the digital certificate in the certificate library using the issuing-party identifier.

6. A method as recited in claim 1 further including accessing the digital certificate in the certificate library using a merchant-specific identifier.

7. A method as recited in claim 1 further including determining which party signed the encrypted second data set by retrieving a public key from another digital certificate.

8. A method as recited in claim 7 further including decrypting the encrypted second data set and comparing the decrypted second data set with the second data set.

9. A method as recited in claim 1 further including presenting a text string to be signed by the corresponding private key.

10. A method as recited in claim 1 further including laying down a cryptographic infrastructure before the issuing party issues the digital certificate, wherein the cryptographic infrastructure includes:

generating and authenticating the user public key and corresponding private key;

creating the certificate library; and

allocating the user-allotted memory segment.

11. A method as recited in claim 10 further comprising minting and distributing a chip card to a user.

12. A method as recited in claim 1 wherein the certificate library is a Lightweight Directory Access Protocol (LDAP) server.

13. A method of authenticating a user presenting a chip card to an entity, the method comprising:

reading a certificate library address from the chip card;

accessing a certificate library memory segment using the certificate library address;

searching the certificate library memory segment for a digital certificate having an entity identifier and followed by a digital certificate chain; and

traversing the digital certificate chain beginning with the digital certificate tagged by the entity identifier until a trusted root certificate is reached.

14. A method as recited in claim 13 further including storing a user private key and the certificate library address on the chip card.

15. A method as recited in claim 13 wherein the certificate library is a Lightweight Directory Access Protocol (LDAP) server.

16. A method as recited in claim 13 further including storing additional digital certificates having different entity identifiers at the certificate library memory segment.

17. A method as recited in claim 16 further including associating additional digital certificate chains with the additional digital certificates, each certificate chain having its own trusted root.

18. A method as recited in claim 13 wherein searching the certificate library memory segment for a digital certificate further includes using specific parameters further specifying which portion of the certificate library memory segment contains a digital certificate issued by the entity.

19. A certificate library having a plurality of user-specific memory segments, each user-specific memory segment storing a plurality of digital certificates issued to a user, each digital certificate identifiable by an issuer-identifier and being associated with a trusted root certificate and each digital certificate having the same user public key.

20. A computer-readable medium containing programmed instructions arranged to authenticate a user presenting a chip card to an entity, the computer-readable medium including programmed instructions for:

reading a certificate library address from the chip card;

accessing a certificate library memory segment using the certificate library address;

searching the certificate library memory segment for a digital certificate having an entity identifier and followed by a digital certificate chain; and

traversing the digital certificate chain beginning with the digital certificate tagged by the entity identifier until a trusted root certificate is reached.